参照 CC 标准的 MAS 安全框架研究及评价

Security Frame and Evaluation in Mobile Agent System

王素贞　(军械工程学院 石家庄 050003)
(河北经贸大学 石家庄 050091)
王嘉祯　(军械工程学院 石家庄 050003)
刘爱珍

摘要:本文提出了面向安全需求达到“足够安全”的定义,给出了一种 Mobile Agent System 主机和代理双向保护的安全框架模型,并给出了 MAS 安全性能评价思路与方法。

关键词:移动 Agent 系统 足够安全 安全框架 评价

1 引言

移动代理 MA (Mobile Agent)本质上是能在异构网络环境中自主移动执行并与环境交互以完成用户特定任务的软件实体,包括移动代码、数据和执行状态。它是由人工智能领域的 agent 技术和网络环境下的分布式技术相结合的产物。MA 技术比移动代码、移动对象技术有了本质上的跨越。MA 在主机上“指定”区域内运行,这个区域称之为平台 MAP(mobile agent platform),它是驻留在主机节点上的一个服务软件实体。网络中的多个主机和其他能与之交互的实体集合构成 MA 的执行环境 EE(execution environment)。MA 和 MAP 构成移动代理系统 MAS(Mobile Agent System)。

2 MAS 安全成因分析与足够安全定义

2.1 MAS 安全问题成因分析

2.1.1 存在系统脆弱性(Vulnerability)

由于计算机单机系统和网络系统均存在脆弱性[4],导致 MAS 具有系统脆弱性,脆弱性是系统固有的属性、不可能完全消除。恶意主体(攻击者或攻击程序)可利用脆弱性获得对系统资源的非授权访问或故意对系统造成损害。MAS 中脆弱点的宿主可以是软件、硬件、协议和标准等,其形成原因是多方面的。

2.1.2 存在系统攻击者(malicious body)

MAS 安全问题的第二个根源是存在系统攻击者。任何系统安全问题本质上是“防护”与“攻击”这一对矛盾,MAS 系统也不例外。我们在研究 MAS 安全策略、安全措施与安全技术的同时,必须深入研究攻击者的行为[5]。安全技术是针对攻击行为的,二者是“相互对抗”、“此消彼长”的关系。攻击者一般情况下的攻击步骤是:

(1) 产生攻击动机,选择攻击目标;

(2) 收集目标信息,寻找目标系统漏洞(脆弱点及宿主);

(3) 对目标实施攻击;

(4) 继续收集信息,实施攻击升级……。沿着从攻击起点到攻击目标这一攻击路径,可将对 MAS 的威胁来源划分为四类:来自通信线路的威胁、来自 MA 的威胁、来自 MAP 的威胁和来自主机的威胁。无论是对主机还是对 MA 的保护,都要充分考虑攻击路径才能阻断攻击。

2.1.3 与实际应用相关(application property)

MAS 安全问题根源之三是系统数据和计算过程的敏感性。实际应用中的 MAS 安全需求是多层次的或者说是多级别的,一个公开的通用系统不需要太强的安全保护,但在商用和军用 MAS 中则需要严格的安全措施。可见,系统脆弱性的危险程度,攻击者的攻击强度都与 MAS 应用系统的性质密切相关。

2.1.4 MAS 足够安全定义(enough security)

面向系统安全需求,本文给出 MAS 足够安全的定义如下:在权衡代价和效果的前提下,如果一个 MAS

系统的安全机制能够与系统安全需求达到最佳匹配，则我们说这个 MAS 是足够安全的。

3 MAS 主要安全技术分析

3.1 主机安全技术及分析

保护主机的技术是传统网络安全技术的扩展，主要有[3]：

(1) 沙箱技术(sand－boxing)，其工作原理是基于软件的错误隔离方法，把不可信的 MA 代码隔离在单独的虚拟地址空间里运行，限制 MA 对本地资源的访问权限，以达到保护主机的目的；其局限性是无法进行内存、CPU 和网络资源直接管理。

(2) 安全代码解释(safe code interpretation)，MAS 系统通常是用解释语言开发的，如 Java、Safe Tcl 等，系统安全策略通过解释器实现，违反安全策略的恶意代码将无法通过解释器的解释而被拒绝执行；其优势是构造多个基于安全策略的解释器可灵活地使用计算资源。

(3) 代码标识(signed code)，用数字签名对代码进行标识是保护主机的一种基本技术，用来验证代码或对象来源的真实性和完整性；该方法依赖公开密钥基础设施。

(4) 授权和属性证书(authorization and attribute certificates)，属性证书中含有权利及其委派方针，应用难点是还未解决怎样表达权利和委派方针，使得证书简单易用。

(5) 状态评价(state appraisal)平台 MAP 使用状态评价函数来确认进入平台的 MA 的状态是否正确(是否被修改过)，并由此决定赋予 MA 多大的权限；此方法的局限性是，评价函数对典型攻击容易模拟识别，而对精巧攻击难以识别。

(6) 历史路径记录(path history)，该方法的核心思想是保留 MA 所访问过的平台的可鉴别的记录，要访问的新平台根据该记录决定应给 MA 怎样的资源限制；其局限性是，随着路径记录的增加，路径校验的代价将变得很高。

(7) 携带验证代码(proof carrying code)，该技术使主机操作系统内核能够验证到达的 MA 是否符合一套安全规则，若符合，则分配给资源，允许执行；未解决的难点是安全策略的形式化和验证的自动化问题。

(8) 携带模式的代码(model－carry code)，该方法是通过引入程序模式来弥补低层次的字节码和高层次的安全策略之间的距离，通过检查模式的正确性和模式是否遵守安全策略来保护运行主机，它有良好的扩展性，但还不能完全解决安全策略的重置问题。在 MAS 安全框架设计时，并不需要一起使用上述的所有的技术，而是要针对实际应用需求，选择几种优化集成到系统中。

3.2 代理安全技术及分析

保护 MA 的主要技术有[3,6]：

(1) 部分结果密封(partial result encapsulation)，基于 RSA 加密方法，采用滑行加密技术(sliding encryption)可实现小尺寸明文加密生成小尺寸密文，可用来保护数据的完整性和机密性。

(2) 探测体(detection object)，它是随机代码段，嵌入 MA 中，探测 MA 是否被修改，用来保护数据的完整性。

(3) 复制和表决(replication and voting)同一 MA 被复制分发到多个主机上，执行完毕通过表决确定最终结果；用来保护计算完整性。

(4) 探测篡改(tamper detection)，使用基于密码的完整性证明或完整性线索确保计算是按照 MA 的指令进行的。

(5) 阻止篡改(tamper proofing)，该类方法把 MA 设计成只有输入输出的黑盒子，其代码和数据不可读取，使恶意主机无法实施对计算过程的窜改。

(6) 加密函数计算(computing with encrypted functions)这种技术对 MA 从算法上保护，如果 MA 想计算 f(x)，只让主机计算加密函数 E(f)(x)，然后 MA 再还原为 f(x)，主机无法知道 MA 的功能。

(7) 环境密钥生成(environmental key generation)，MA 在预定义环境为真时，生成密钥对代码密文解密，使得恶意主机无法直接读取代码来了解 MA 的行为。

(8) 嵌套式执行环境(nested environments)，代理自己提供运行环境而不直接在主机上运行，由三部分组成：MA 本身、MA 载体和 MA 解释器。

(9) 防窜改硬件(tamper－proof hardware)，依赖硬件构成防窜改环境，MA 可以存储和运行在被隔离被保护的环境中，基本可杜绝各种软件攻击。

4　参照 CC 标准的 MAS 安全框架

4.1　安全功能

在 CC 标准中，安全功能需求以类→族→组件的形式进行定义。MAS 主要安全需求有：

（1）安全审计，对有关的操作信息识别、记录、存储和分析；

（2）安全通信，确保数据交换双方的身份，防止收发任一方抵赖；

（3）加密支持，包括密钥管理和加密操作等；

（4）用户数据和用户隐私保护；

（5）身份识别与认证；

（6）资源可用性支持等。

4.2　MAS 安全框架模型

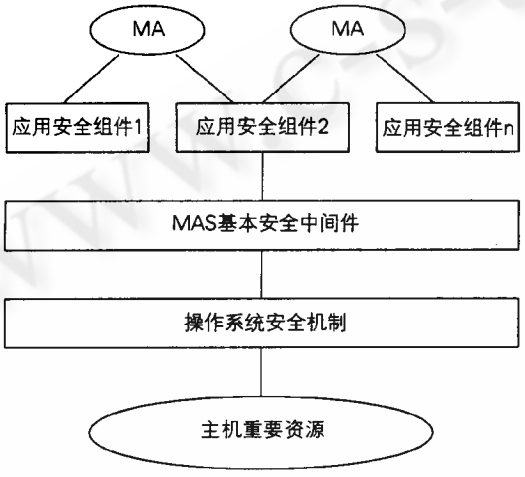

图 1　通用 MAS 安全框架

MAS 安全机制可分层实施，如图 1 所示。第一层是可访问的网络主机资源，它需要安全保护；第二层是标准的操作系统安全机制，在此基础上要加强，虽然在上层可使用沙箱（user – level sandboxing）技术，可以把 MA 限制在只对某些资源的访问的范围内，但是研究表明沙箱技术也具有脆弱性，某些恶意 MA 可利用之进行系统调用，因此，在这一层可以使用系统调用拦截（system call interception）加强安全，例如在 Linux 操作系统使用 jailing 技术，确保恶意 MA 不能绕过中间件安全机制而直接调用操作系统。第三层是 MAS 通用中间件安全机制，对主机和对 MA 的基本保护在该层可部分实现。例如，MA 要在上下文（context）中执行，利用沙箱技术对上下文限制，使之只能与上层应用安全组件通过已经定义好的通道（channel）连接，在指定的域内执行，MA 则不能创建受控通道以外的连接。同时，有选择地使用较成熟的保护 MA 的技术，对 MA 实施完整性、私有性保护。第四层是应用安全组件，对于不同应用类型的 MA 和主机，可以选择调用相应的安全组件以定制具体的安全需求。由于 Java 有较好的安全机制。图 2 给出了一个基于 Java1.3/1.4 安全特性的 MAS 安全框架模型，既能实现主机与代理的隔离，又能实现主机和代理的双向保护。

4.3　安全技术与攻击类型的初步匹配

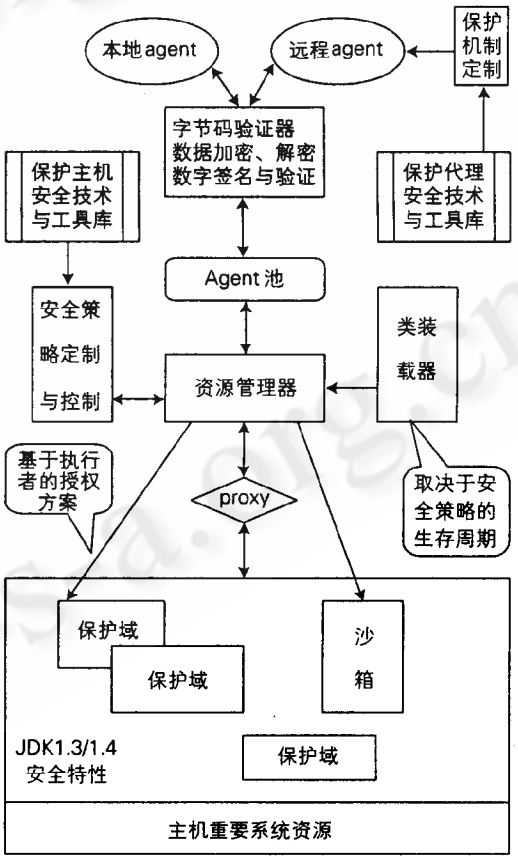

图 2　基于 JDK 的 MAS 双向保护安全框架

由以上分析可知，目前已有多种保护主机和 MA 的技术可用于 MAS 的安全设计，但多数不够成熟，彼此之间不一定是相容的，也没有一种技术是适合所有应用场合的。有必要对已有的和新出现的多种安全技术进行实验、分析和评价，建立安全需求、攻击类型与

安全技术有效匹配的数据库，形成一些方便 MAS 用户应用开发的安全组件。表 1 从分析安全机制入手，给出安全技术遏制攻击类型的初步匹配，更充分的匹配信息有待于进一步实验并分析得出。

表 1　攻击类型与安全技术初步匹配

攻击类型		安全技术
代理对平台 (Agent – to – Platform)	伪装(Masquerading)	身份认证，代码标识 携带验证代码
	拒绝服务 (Denial of Service)	授权和属性证书 (使用电子货币)有尝服务
	非授权访问 (Unauthorized Access)	认证、授权，沙箱技术 安全代码解释
	复制与重放 (Copy and Reply)	状态估计 (使用有效时间戳)
平台对代理 (Platform – to – Agent)	伪装(Masquerading) 拒绝服务 (Denial of Service)	部分结果密封、探测恶意主机 复制和表决 环境密钥生成
	监听(Eavesdropping) 篡改(Alteration)	篡改阻止、有限时间黑箱、计算功能加密、嵌套的执行环境等
代理对代理 (Agent – to – Agent)	非授权访问 (Unauthorized Access)	代理认证、授权
	拒绝服务 (Denial of Service)	相互授权 状态报告
	伪装(Masquerading)	代理认证
	抵赖(Repudiation)	数字签名

5　系统安全评价初步

目前，尽管 MAS 的应用前景看好，但由于 MAS 处在系统实验阶段还没有广泛实际应用，国内外还没有形成 MAS 安全性能评价的方法，也几乎看不到有关这方面的理论和应用研究。本文参考 CC 标准并考虑到我国的实际情况，认为 MAS 安全功能的可信度评价应针对 MAS 应用系统实际安全需求来进行，在系统设计、开发、测试和运行阶段都应该考虑进去，可用安全等级、安全系数等来定性描述和定量刻画 MAS 安全程度，具体列出每个安全等级上可抵御的攻击，对于每一个投入使用的 MAS，都应当给出一个安全功能可信度评价结果。下面仅给出一个粗略的评价思路。

5.1　安全性能评价

操作思路：

(1) 列出 MAS 应用系统中主机和 MA 安全需求一级指标及其二级指标，一级可表示为等级描述，二级可表示为量化数值；

(2) 评估并记录在设计、开发、测试、运行各个阶段安全需求的实现程度，并以同样的数据结构给出，便于比较；(3) 给出安全指标相对应的优化方向，及安全性能提升空间与要付出的代价增量。

(4) 检测系统脆弱性，并进行风险程度评估与描述。

(5) 建立 MAS 安全性能评估距阵，对此进行加权处理。可得出系统安全程度。

5.2　安全代价分析

若追求 MAS 极端安全状态，必将导致系统复杂度增加、工作效率降低，安全代价增高。本文的出发点是根据实际需求实现足够安全，逼近系统的安全机制与系统安全需求最佳匹配的状态，寻找安全代价和安全效果的平衡点。作者在利用 Java 语言自开发的基于组件的 MAS 原型系统中开始实验探索提升安全级别与增加安全代价的关系。

6　结束语

本文分析了 MAS 安全问题形成的原因，分析比较了现有的保护主机和保护代理的各种技术的优缺点，面向安全需求，给出了足够安全的定义，提出了一个 MAS 平台和代理双向保护的安全框架模型，并给出了 MAS 性能安全评价的思路与方法。

参考文献

1 谢希仁，计算机网络(第四版)[M]，北京 电子工业出版社，2004.2。

2 郑人杰等，实用软件工程(第二版)[M]，北京 清华大学出版社，2001.10。

3 Wayne Jansen，Tom Karygiannis. NIST Special Publication 800 – 19 – Mobile Agent Security. http // www. Nist. gov.

4 冯兵，网络安全脆弱性综合测评方法与应用研究，PhD. 2004.12。

5 王汝传等，移动代理安全性研究综述[J]，重庆邮电学院学报(自然科学版)，2004.3(81 – 86)。

6 侯方勇等，移动代理防范恶意主机安全技术研究，计算机应用研究，2004．9。